MEMORANDUM FOR: Suzanne E. Spaulding
Under Secretary for National Protection and Programs Directorate

FROM: Jeh Charles Johnson

SUBJECT: Designation of Election Infrastructure as a Subsector of the Government Facilities Critical Infrastructure Sector

I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, certain systems and assets of election infrastructure meet the statutory definition of critical infrastructure in fact and in law.

I have reached this determination so that election infrastructure, on a more formal and enduring basis, continues to be a priority in the cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," I mean at least the information, capabilities, physical assets, and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections. Election infrastructure is inclusive of but not limited to the following components.

- Physical locations:
  - Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.
  - Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
  - Centralized vote tabulation locations, which are used by some States and localities to process absentee and Election Day voting materials.

- Information and communication technology (ICT):
    - Information technology infrastructure and systems used to maintain voter registration databases.
    - Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
    - Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of State governments, as well as for postelection reporting used to certify and validate results.

I direct the National Protection and Programs Directorate (NPPD) to institutionalize the Election Infrastructure subsector in the Government Facilities sector under the National Infrastructure and Protection Plan (NIPP) and incorporate the subsector into the NIPP framework. An NPPD serves as a Sector Specific Agency for the Government Facilities sector, I also direct NPPD to serve as the Sector Specific Agency for the Election Infrastructure subsector on behalf of DHS.

Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems. Election infrastructure is vital to our national interests. This designation enables the states, should they request it, to leverage the full scope of cybersecurity services available to them.

- **Election Infrastructure Subsector Q&As**

Q: What is the process by which DHS establishes a critical infrastructure sector?

- Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* directs the Secretary of Homeland Security to evaluate the need for, and approve changes to, critical infrastructure sectors. The only requirement in this process is that the Secretary shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated Sector-Specific Agency for that sector. The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Q: Can this decision be reversed by the next Administration?

- Future Administrations may outline similar authorities regarding the structure and organization of critical infrastructure sectors, however, unless amended, the definition of “critical infrastructure” will remain as provided in the USA Patriot Act of 2001, as amended.

- Designations of critical infrastructure sectors are addressed in Presidential Policy Directive 21. Future Administrations may institute their own policy directives.

- We note that Administrations often choose to leave policy directives from previous administrations in place and update them as needed. For example, PPD-21, signed February 2013, replaced Homeland Security Presidential Directive 7 (Critical Infrastructure Identification, Prioritization, and Protection), issued in December 2003. DHS’s Critical Infrastructure work spans administrations, pre-dating the Department with the Clinton administration, becoming formalized under the George W. Bush administration, then adapted and updated by the Obama administration.

Q: Are there any carve-outs or safe harbors that states could employ to exempt them from a designation?

- All participation, including receipt of services and engagements with sector coordinating council is entirely voluntary.

Q: What would establishing a critical infrastructure sector or subsector mean for the elections community?

- First, it is important to note that **all participation is entirely voluntary** in any of the offerings for critical infrastructure stakeholders. If your state or jurisdiction does not want to leverage any of the services or benefits DHS provides to the critical infrastructure community, DHS will not compel you to do so. Establishing a critical infrastructure subsector for elections **does not involve Federal intrusion, takeover, or regulation** of any kind. Rather, establishment provides the benefit of certain protections and services that are voluntary and upon request.

- Second, the existing technical assistance services that several states are taking advantage of will continue. These include the following services for which states have reported very positive feedback:
  - **Cyber Hygiene scans on Internet-facing systems**: These scans can provide election officials with a report identifying vulnerabilities and mitigation recommendations to improve their cybersecurity posture, and
  - **Risk and Vulnerability Assessments (RVAs)**: These assessments include a wide range of penetration testing services, application, and database testing.

- Establishment of election infrastructure as a critical infrastructure subsector would enable DHS to prioritize its assistance to election officials in three phases:
  1. Reduce system vulnerabilities
  2. Understand threats to election infrastructure
  3. Respond to incidents and malicious cyber actors

  Reduce system vulnerabilities

  Designation as sub-sector establishes mechanisms to rapidly share information across the community to identify and mitigate system vulnerabilities.

  1. Designation as a sub-sector would support the establishment of a **sector coordinating council** focused on the security and resilience of the election infrastructure. Coordinating councils are used to share information on vulnerabilities and threats and to enable collaboration across Federal, state, and local governments, as well as with private sector partners, to determine ways to mitigate risks. Participation in the council is voluntary.

  2. A sub-sector would be covered by the **Critical Infrastructure Partnership Advisory Council (CIPAC))** framework, so that DHS could convene meetings with state and local election officials, and these meetings could be closed to the public and exempt from FACA requirements.

Order 13694 would be able to sanction persons responsible for cyber enabled activities that harm or compromise a computer that supports an entity in a critical infrastructure sector.

Last month, this Executive Order was amended to enable the Secretary of Treasury to also be able to sanction persons responsible for cyber enabled activities that tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions. This amendment was added because of Russian activities related to the 2016 U.S. election. Establishing a sub-sector for election infrastructure would enable the Executive Order to be used against actors that intend to harm or compromise election systems more broadly, including for theft of personal information involving a computer that supports an entity in a critical infrastructure sector, for example, that undermines confidence in the confidentiality of voter registration databases and, thereby, may lead to lower the public's willingness to register. These protections may serve to deter future malicious cyber behaviors or allow the U.S. government to hold cyber actors accountable for their actions.

3. **Protected Critical Infrastructure Information** (PCII). Additionally, developers and operators of infrastructure can voluntarily share critical information with DHS under a **protection of critical infrastructure information (PCII)** statute that protects information from Freedom of Information Act (FOIA) requests, use in civil litigation, and regulatory use. [1] In practice, this means that states, vendors, or individuals that identify vulnerabilities in election infrastructure can share this information, to the benefit of all who leverage these systems, without fear that it will be used against them. This, in combination with the heightened awareness of vulnerabilities through the sector coordinating council, provides an effective mechanism for a state that learns of and remediates a vulnerability to take steps to ensure that their mitigation solution can be applied to all other states and localities impacted by the same vulnerability.

Understand threats to election infrastructure

Additionally, as a critical infrastructure subsector, DHS would be able to prioritize providing **security clearances to election officials** as appropriate. This would enable election officials to be briefed on relevant classified intelligence, and to secure their systems in a manner more informed of the threats they face. In other sectors, this type of information is especially valuable in the engineering, design, and procurement decisions among the sector.

Respond to incidents and malicious cyber actors

DHS provides funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC)**.** States already have access to the **cyber incident response capabilities of the MS-ISAC,** however, historically, much of the MS-ISAC's attention has focused on the work of the Chief Information Officers and Chief Information Security Officers for each state's overall systems and networks. As a critical infrastructure subsector, election officials' incident response needs and requests for services can be prioritized, both by DHS and MS-ISAC, over requests from non-critical infrastructure stakeholders.

- Lastly, owners and operators of election infrastructure in a designated subsector would benefit from the U.S. government's **strategic efforts to protect critical infrastructure**, including the promotion of **international norms that prohibit peacetime cyber attacks** against critical infrastructure as well as the use of certain **Executive Orders to respond to attacks** on election infrastructure. As a sub-sector of critical infrastructure, the Secretary of Treasury, under Executive

[1] *See* 6 U.S.C. §133

TICK TOCK:

Friday, January 6: This guidance is shared under embargo with DOJ, FBI and NIST.

Following the release of the IC report:

- + 2 hours; NASS and Congressional leadership staff notifications
- +2.30 hours; OLA notifications to Authorizers and Appropriators
- + 2:45 hours; Embargoed release to other Congressional members
- + 3 hours; Secretary Johnson issues statement
- + 3:30 hours; Stakeholder notifications